Ueber

n^{te} Potenzreste

und

binomische Congruenzen dritten Grades.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

bei der

philosophischen Fakultät
der Ludwig-Maximilians-Universität zu München

vorgelegt von

Jos. Mayer,
K. Gymnasialprofessor in Freising.

Freising.
Buchdruckerei von Anton Fellerer.
1895.

Ueber

n^{te} Potenzreste

und

binomische Congruenzen dritten Grades.

Inaugural-Dissertation

zur

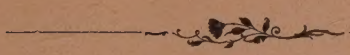
Erlangung der Doktorwürde

bei der

philosophischen Fakultät
der Ludwig-Maximilians-Universität zu München

vorgelegt von

Jos. Mayer,
K. Gymnasialprofessor in Freising.



Freising.
Buchdruckerei von Anton Fellerer.
1895.

Vorwort.

Gelegentlich der Untersuchung über die Werte von x der Congruenz $10^x \equiv 1$ für einen beliebigen reellen Modul, zu welcher mir ausser anderen vor allem die disquisitiones arithmeticae von Gauss, die théorie des nombres von Legendre, die Vorlesungen über Zahlentheorie von Lejeune Dirichlet und Bachmann's Lehre von der Kreisteilung dienten, ergaben sich mir bei der Frage nach den n^{ten} Potenzresten, insbesondere den kubischen Resten reeller Primzahlmoduln manche Sätze und Relationen. Wie nachträgliche Vergleiche zeigten, sind einige derselben allerdings Analoga von Sätzen der disquisitiones arithmeticae. Wo aber solche Anklänge vorhanden sind, versäumte ich nicht, den Zusammenhang nachzuweisen. Uebrigens ist die Beweisführung selbst in diesen Fällen eine wesentlich andere. Wenn ausserdem der im § 1 Kap. I. ausgesprochene Satz auch sonst schon in der Zahlentheorie vorkommt, so hielt ich es doch wegen des Folgenden für nötig, ihn so wie es hier geschehen ist, zu fassen und zu beweisen. Zahlenbeispiele beizufügen, unterliess ich der Kürze halber überall da, wo es nicht unbedingt angezeigt schien, weil sie auf gewöhnliche Weise, in den meisten Fällen aber mittelst des canon arithmeticus von Jacobi leicht gebildet werden können.

Die seinerzeit von mir niedergeschriebenen Notizen über binomische Congruenzen dritten Grades wurden durch die §§ 3, 4, 5, 6 und 7 Kap. II. zu einer Art Theorie derselben erweitert. Ich masse mir nicht an, eine solche erschöpfend gegeben zu haben. Denn dazu würde ich auch die Bestimmung des kubischen Charakters einer reellen Zahl rechnen. Aber schon Gauss hatte vergeblich versucht, das kubische

Reciprocitätsgesetz für reelle Primzahlen nachzuweisen. Wohl lässt sich ein Satz aufstellen, der eine Erweiterung des von Gauss zur Stütze seines 3ten Beweises des quadratischen Reciprocitätsgesetzes ausgesprochenen Lemmas ist, und auf Grund desselben einen Ausdruck für den kubischen Charakter einer Zahl mittels des kubischen Charakters der Zahl 2 finden. Allein wenn die praktische Anwendung jenes Lemmas zur Bestimmung des quadratischen Charakters einer Zahl schon innerhalb sehr beschränkter Grenzen liegt*) (s. z. B. meine Ausführungen über die Bestimmung des quadratischen Charakters der Zahlen 2 und 5 in den §§ 17 und 18 meiner oben angegebenen Abhandlung), so ist dieses um so mehr der Fall bei der Bestimmung des kubischen Charakters mittels des analogen Satzes. Die Aufnahme dieses und vollends des schon von Jacobi und Eisenstein bewiesenen Reciprocitätsgesetzes für kubische Reste von zwei primären Primzahlen von der Form $a + b\varrho$, wo ϱ eine der beiden imaginären Wurzeln der Einheit ist, würde den Rahmen dieses Schriftchens, in welchem nur reelle ganze Zahlen behandelt werden sollen, überschreiten.

Auch verkenne ich nicht, dass trotz meiner eifrigen Suche nach etwa schon vorhandenen Schriften über dieses specielle Thema doch nicht irgendwo Aehnliches behandelt worden sein könnte. Dass ich bei dieser Suche ziemlich weit ausgeholt habe, dürfte allein schon aus den Citaten der vorher erwähnten Abhandlung, die indessen durchaus nicht Alles anführen, was berücksichtigt wurde, und zum Teil auch dieser ersehen werden.

---

*) Vor kurzem ist eine Inauguraldissertation erschienen über die Bestimmung des Wertes von μ in dem Gauss'schen Lemma, die ich mir leider vor Drucklegung dieser Schrift nicht verschaffen konnte, um den Inhalt derselben einsehen und den Titel genau angeben zu können.

I. Kapitel.

Ueber n^{te} Potenzreste.

§ 1.

In der Congruenz $x^n \equiv a \pmod{p}$ sei x die Unbekannte und die beliebige Zahl a durch die Primzahl p nicht teilbar; ferner haben n und p—1 den grössten gemeinschaftlichen Teiler q, sodass, wenn $n = n'q$ und $p - 1 = p'q$ gesetzt wird, n' und p' relative Primzahlen sind. Dann ist, wenn vorstehende Congruenz möglich ist, $a^{p'} = a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$.

Bew. Wenn es ein x giebt, welches der Congruenz

$$x^n \equiv a \pmod{p} \text{ oder}$$

$$x^{n'q} \equiv a \pmod{p} \text{ genügt, so ist auch}$$

$$x^{n'qp'} \equiv a^{p'} \pmod{p}.$$

Weil aber nach dem Fermat'schen Satze für jede durch p nicht teilbare Zahl x

$$x^{p'q} = x^{p-1} \equiv 1 \pmod{p}, \text{ also auch}$$

$$x^{n'qp'} \equiv 1 \pmod{p}, \text{ so ist auch}$$

$$a^{p'} = a^{\frac{p-1}{q}} \equiv 1 \pmod{p}.$$

Umgekehrt: Wenn a eine beliebige durch die Primzahl p nicht teilbare Zahl, $n = n'q$ und $p - 1 = p'q$, wobei n' und p' relative Primzahlen sind, und $a^{p'} \equiv 1 \pmod{p}$, so ist die Congruenz $x^n = x^{n'q} \equiv a \pmod{p}$ immer möglich und zwar hat sie q reelle Wurzeln.

Bew. Es sei g eine primitive Wurzel von p und

$a \equiv g^{\alpha} \pmod{p}$. Dann ist

$a^{p'} \equiv g^{\alpha p'} = g^{\alpha \cdot \frac{p-1}{q}} \equiv 1 \pmod{p}$, d. h.

α muss durch q teilbar, also $= \alpha' q$ sein.

Setzt man ferner $x \equiv g^{\xi} \pmod{p}$, so folgt

$x^n \equiv g^{n\xi} \equiv g^{\alpha} \pmod{p}$, mithin

$n\xi \equiv \alpha \pmod{p-1}$.

Nun haben n und p—1 den grössten gemeinschaftlichen Teiler q. Derselbe ist nach Obigem auch in α enthalten; daher hat diese Congruenz q Wurzeln, mithin giebt es auch q Werte von ξ, welche q verschiedene Werte von x liefern.

Zusatz 1) Sind n und p—1 relative Primzahlen, so ist die Congruenz

$x^n \equiv a \pmod{p}$ immer möglich, weil immer

$a^{p-1} \equiv 1 \pmod{p}$, und zwar giebt es nur eine Wurzel dieser Congruenz.

Zusatz 2) Ist n' prim zu p—1 d. i. zu q, so giebt es eine primitive Wurzel γ, welche von der Art ist, dass

$\gamma^{n'} \equiv g \pmod{p}$.

Es ist alsdann $(\gamma^{n'})^{\alpha'} \equiv g^{\alpha'} \pmod{p}$ oder

$(\gamma^{\alpha'})^{n'} \equiv g^{\alpha'}$ „ , also auch

$(\gamma^{\alpha'})^{n'q} \equiv g^{\alpha' q}$ „ oder

$(\gamma^{\alpha'})^{n'q} \equiv a \pmod{p}$ d. i. eine Wurzel der

Congruenz ist $x \equiv \gamma^{\alpha'} \pmod{p}$.

§ 2.

Sind $a_1, a_2, \ldots$ die n^{ten} Potenzreste einer Primzahl p und haben n und p—1 den grössten gemeinschaftlichen Teiler q, so ist das Produkt dieser Potenzreste $\equiv +1 \pmod{p}$, wenn $\frac{p-1}{q}$ ungerade, hingegen $\equiv -1 \pmod{p}$, wenn $\frac{p-1}{q}$ gerade ist.

Bew. Die Anzahl der n^{ten} Potenzreste ist $\frac{p-1}{q} = p'$.

Sie sind nämlich die Wurzeln der Congruenz

$$x^{p'} \equiv 1 \pmod{p}.$$

Ausser diesen Wurzeln giebt es keinen n^{ten} Potenzrest von p. Diese Congruenz hat aber, weil p' und $p-1$ den grössten gemeinschaftlichen Teiler p' haben, nach § 1 p' Wurzeln, nicht mehr und nicht weniger.

Ist nun g eine primitive Wurzel von p und

$$\begin{aligned} a_1 &\equiv g^{\alpha_1} \pmod{p} \\ a_2 &\equiv g^{\alpha_2} \quad \text{„} \\ a_3 &\equiv g^{\alpha_3} \quad \text{„} \\ &\cdots\cdots \\ a_{p'} &\equiv g^{\alpha_{p'}} \quad \text{„} \quad \text{, so ist} \end{aligned}$$

$$a_1 \cdot a_2 \cdot a_3 \cdots a_{p'} \equiv g^{\alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_{p'}} \pmod{p}.$$

Nun muss nach § 1

$$\begin{aligned} \alpha_1 &= q\alpha_1' \\ \alpha_2 &= q\alpha_2' \\ &\cdots\cdots \\ \alpha_{p'} &= q\alpha_{p'}' \text{ sein, daher ist} \end{aligned}$$

$$\alpha_1 + \alpha_2 + \cdots + \alpha_{p'} = q\,(\alpha_1' + \alpha_2' + \cdots + \alpha'_{p'}).$$

Wenn $\alpha_1, \alpha_2, \ldots \alpha_{p'}$ die kleinsten positiven Potenzreste (mod. p) sind, so stellt die Summe $\alpha_1' + \alpha_2' + \ldots + \alpha'_{p'}$ die Summe $1 + 2 + \ldots + p' = (1 + p')\frac{p'}{2} = \left(1 + \frac{p-1}{q}\right)\frac{p-1}{2q}$ dar.

Daher ist $a_1 \cdot a_2 \cdots a_{p'} \equiv g^{q\left(1 + \frac{p-1}{q}\right)\cdot\frac{p-1}{2q}} \pmod{p}$ oder $\equiv g^{\frac{p-1}{2}\left(1 + \frac{p-1}{q}\right)} \pmod{p}$.

Aber $g^m \cdot \frac{p-1}{2} \equiv \pm 1 \pmod{p}$, je nachdem m eine gerade oder ungerade Zahl ist. Mithin ist das genannte Produkt $\equiv \pm 1 \pmod{p}$, je nachdem $1 + \frac{p-1}{q}$ gerade oder ungerade ist.

§ 3.

Unter diesen Zahlen $a_1, a_2, \ldots a_{p'}$ sei eine a_μ, welche

zum Exponenten p' gehört. Denn unter den Wurzeln der Congruenz $x^{p'} \equiv 1 \pmod{p}$ kommen alle Zahlen vor, welche zu $p' \pmod{p}$ gehören. Es sind nämlich die Potenzen $a_\mu, a_\mu^2, \ldots . a_\mu^{p'}$ alle incongruent, aber auch Wurzeln der Congruenz $x^{p'} \equiv 1 \pmod{p}$, daher ihre kleinsten positiven Reste identisch mit $a_1, a_2, \ldots a_{p'}$, wenn auch in verschiedener Aufeinanderfolge. Diese kleinsten positiven Reste bilden aber eine Periode von Resten, da sie sich wiederholen, wenn man die Potenzen von a_μ über die p'^{te} hinaus fortsetzt. Mithin ist in § 2 bewiesen, dass, wenn a_μ zu p' gehört, das Produkt $a_\mu \cdot a_\mu^2 \ldots . a_\mu^{p'} \equiv \pm 1 \pmod{p}$, je nachdem p' ungerade oder gerade ist.

Der in § 75 der disquisitiones arithmeticae von Gauss aufgestellte Satz handelt also von denselben Zahlen, von welchen in § 2 die Rede ist.

§ 4.

Ist $p' = \frac{p-1}{q}$ eine gerade Zahl, wo q dieselbe Bedeutung wie oben hat, so lassen sich die n^{ten} Potenzreste zu Paaren gruppieren, deren Summen $= 0$ od. $= p$ sind, je nachdem man die absolut- od. positiv kleinsten Reste (mod. p) nimmt.

Bew. Wenn p' gerade und $a_\mu^{p'} \equiv 1 \pmod{p}$, so ist auch

$$(-a_\mu)^{p'} \equiv 1 \pmod{p},$$ daher

$a_\mu + (-a_\mu) = 0$ oder $a_\mu + (p - a_\mu) = p$.

Z. B. Ist $n = 3, 5, 7, \ldots .$ und p bzw. von der Form $6m + 1, 10m + 1, 14m + 1, \ldots .$, so ergänzen sich immer je zwei Potenzreste zu 0 oder p.

§ 5.

Der in § 4 angeführte Satz lässt sich für besondere

Werte von p' noch enger fassen. Ist nämlich $p' = 2^\mu p''$, wo μ eine beliebige ganze Zahl, aber > 1, und p'' eine ungerade Zahl ist, so kann man die **zu p' gehörigen Zahlen** in Paaren ordnen, deren Summen $= 0$ bzw. $= p$ sind.

Bew. Die Anzahl der Zahlen, welche zu $p' = 2^\mu p''$ gehören, ist $\varphi(2^\mu p'')$ und eine gerade Zahl. Es sei eine derselben a_ν; dann kommen sie alle unter den kleinsten Resten der p' Potenzen $a_\nu, a_\nu^2, \ldots . a_\nu^{p'}$ vor, weil alle Potenzen von a_ν^1 bis $a_\nu^{p'}$, deren Exponenten relativ prim zu p' sind, zu p' gehören und sonst keine.

Gehört nun a zu 2^μ (mod. p), so gehört auch $-$ a zu 2^μ (mod. p). Denn jedenfalls ist wegen $a^{2^\mu} \equiv 1$ (mod. p) auch

$$(-a)^{2^\mu} \equiv 1 \text{ (mod. p)}.$$

Würde $-$ a zu einem kleineren Exponenten gehören, so müsste dieser ein Teiler von 2^μ, also von der Form $2^{\mu'}$ sein, wo $\mu' < \mu$ ist. Dann wäre

$$(-a)^{2^{\mu'}} \equiv 1 \text{ (mod. p) oder}$$

$(-1)^{2^{\mu'}} . a^{2^{\mu'}} \equiv 1$ (mod. p). Weil aber $(-1)^{2^{\mu'}}$ wegen $\mu' > 0$ stets $\equiv 1$ (mod. p), so müsste gegen die Voraussetzung

$$a^{2^{\mu'}} \equiv 1 \text{ (mod. p) sein.}$$

Da 2^μ und p'' relative Primzahlen sind, so gehören, wenn $a_1, a_2, \ldots .$ zu p'' (mod. p) gehören, auch $aa_1, aa_2, \ldots$ und $-aa_1, -aa_2, \ldots .$ zu $2^\mu p''$ (mod. p)*).

Zusatz. Zu $2^\mu = 2^1$ gehört immer nur $p - 1$ und ausserdem keine Zahl. Allerdings hat $x^2 \equiv 1$ (mod. p) die beiden Wurzeln 1 und $p - 1$. Allein 1 gehört zu 1. Also

*) Der von Gauss in § 55 der disqu. arithm. für $q = p - 1$ durchgeführte Beweis kann ähnlich auch für jeden anderen Teiler von $p-1$ erbracht werden.

entspricht für $p' = 2^1 p''$ einem $+ a = p - 1$ keine Zahl $= -a$; daher können auch den Zahlen $aa_1, aa_2, \ldots$ keine Zahlen $-aa_1, -aa_2, \ldots$ entsprechen.

Folgerung. Da nach § 4, wenn p' gerade ist, alle der Congruenz $x^{p'} \equiv 1 \pmod{p}$ genügenden Werte sich zu Paaren, die sich zu 0 bzw. p ergänzen, gruppieren lassen und unter diesen, wenn $p' = 2^{\mu} p''$, wo $\mu > 1$, wieder diejenigen, welche zu $p' \pmod{p}$ gehören, so werden in letzterem Falle auch diejenigen, welche nicht zu p' gehören, sich zu Paaren, die sich zu 0 bzw. p ergänzen, zusammenstellen lassen.

§ 6.

Ist a ein n^{ter} Potenzrest, so giebt es ausser 1 immer einen, aber auch nur einen n^{ten} Potenzrest, welcher mit dem ersten multipliciert $\equiv 1 \pmod{p}$ ist.

Beweis. Ist $a^{p'} \equiv 1 \pmod{p}$ und bestimmt man x so, dass $ax \equiv 1 \pmod{p}$, so ist

$$a^{p'} x^{p'} \equiv 1 \pmod{p},$$

also wegen

$$a^{p'} \equiv 1 \pmod{p}$$

auch

$$x^{p'} \equiv 1 \pmod{p}.$$

Es giebt aber auch nur einen solchen n^{ten} Potenzrest, weil nur ein einziger Wert von x der Congruenz $ax \equiv 1 \pmod{p}$ genügt.

Zusatz 1) Ist die eine Zahl eines solchen Paares a und die andere b, so ist, wenn $a_{\mu}^{p'} \equiv 1 \pmod{p}$ und

$$a \equiv a_{\mu}^{m} \pmod{p},$$

$$b \equiv a_{\mu}^{p'-m} \pmod{p}.$$

Zusatz 2) Die Fälle $p' = 1$ und $p' = 2$ sind ausgenommen. Für $p' = 2$ kann a nur $\equiv +1 \equiv -1 \pmod{p}$ sein.

Zusatz 3) Ist p' gerade, so ist, wie wir in § 9 sehen werden, ein Potenzrest $= -1$. In diesem Falle gehört zu $a = -1$ kein davon verschiedener, sondern ist in der Con-

gruenz $ax \equiv 1 \pmod{p}$

$x = a = -1.$

Anmerkung. Die von Euler als socii aufgeführten und von Gauss in § 77 der disqu. arithm. erwähnten Zahlen sind also zugleich n^{te} Potenzreste oder nicht.

§ 7.

Gehört a zu $q > 2$, so giebt es immer ausser 1 eine, aber auch nur eine Zahl, welche zu q gehört und mit ersterer multipliciert $\equiv 1 \pmod{p}$ ist.

Bew. Gehört a zu q, so ist der Wert von x, welcher der Congruenz $ax \equiv 1 \pmod{p}$ genügt, diese Zahl.

Denn 1) ist wegen $a^q \equiv 1 \pmod{p}$ auch

$x^q \equiv 1 \pmod{p}$,

2) ist q aber auch die Zahl, zu welcher x gehört. Denn gäbe es eine kleinere, etwa q', dann würde aus

$ax \equiv 1 \pmod{p}$ folgen

$(ax)^{q'} \equiv 1$ „ oder

$a^{q'}x^{q'} \equiv 1$ „ .

Weil aber $x^{q'} \equiv 1 \pmod{p}$ nach der Annahme, so wäre auch $a^{q'} \equiv 1 \pmod{p}$ gegen die Voraussetzung.

Zusatz. Ebenso wie in § 6 Zus. 1) kann gezeigt werden, dass je zwei zu einem Paare gehörige Zahlen congruent sind den Potenzen einer zu q gehörigen Zahl, deren Exponenten sich zu q ergänzen.

§ 8.

Das Produkt aller zu einem Exponenten $q > 2$ gehörigen Zahlen ist $\equiv 1 \pmod{p}$.

Dieser Satz ist nur eine Folgerung aus § 7 und schliesst den Satz § 80 der disqu. arithm. in sich.

§ 9.

Wenn p' eine ungerade Zahl, so giebt es keinen n^{ten} Potenzrest $\equiv -1 \pmod{p}$.

Denn $(-1)^{p'}$ ist immer nur $\equiv -1 \pmod{p}$.

Zusatz. Gehört a_μ zu einem ungeraden Exponenten q, so kommt in der Restperiode $a_\mu, a_\mu^2, \ldots . a_\mu^q$ kein Rest $\equiv -1$ vor; es giebt daher keine Potenz von a_μ, welche $\equiv -1 \pmod{p}$ ist. Denn wäre

$$a_\mu^\nu \equiv -1 \pmod{p}, \text{ wo } \nu < q \text{ ist, so müsste}$$

$$(a_\mu^\nu)^q \equiv (-1)^q \equiv 1 \pmod{p} \text{ sein, was unmöglich ist.}$$

§ 10.

Ist p' eine gerade Zahl, so giebt es immer einen n^{ten} Potenzrest $\equiv -1 \pmod{p}$ und zwar ist dieser $\equiv a_\mu^{\frac{p'}{2}}$, wenn a_μ zu p' gehört.

Denn es ist $(-1)^{p'} \equiv 1 \pmod{p}$.

Ferner ist $a_\mu^{p'} \equiv 1 \pmod{p}$, also

$$(a_\mu^{\frac{p'}{2}} + 1)(a_\mu^{\frac{p'}{2}} - 1) \equiv 0 \pmod{p}.$$

Weil aber nicht $a_\mu^{\frac{p'}{2}} \equiv 1 \pmod{p}$ sein kann, da sonst a_μ zu einem kleineren Exponenten als p' gehören würde, so muss

$$a_\mu^{\frac{p'}{2}} \equiv -1 \pmod{p} \text{ sein.}$$

Zusatz. Aus den §§ 6, 9 und 10 folgt: das Produkt aller n^{ten} Potenzreste ist $\equiv \pm 1 \pmod{p}$, je nachdem p' ungerade oder gerade ist. (S. § 2!)

§ 11.

Sind a_μ und a_ϱ n^{te} Potenzreste, welche zu p' gehören, und ist ausserdem $a_\mu . a_\varrho \equiv 1 \pmod{p}$, so folgen die Reste aufeinanderfolgender Potenzen von a_μ in umgekehrter Ordnung wie die Reste der Potenzen von a_ϱ.

Bew. Unter den Potenzen von a_μ muss eine einer Potenz von a_ϱ congruent sein (§ 3), also etwa

$a_\mu^\alpha \equiv a_\varrho^\beta \equiv r \pmod p$. Dann ist auch

$a_\mu^{\alpha+\nu} \equiv r a_\mu^\nu \pmod p$ und, da

$r \equiv a_\varrho^\beta \pmod p$, so ist auch

$a_\mu^{\alpha+\nu} \cdot r \equiv r \cdot a_\mu^\nu \cdot a_\varrho^\nu \cdot a_\varrho^{\beta-\nu} \pmod p$.

Weil aber nach der Voraussetzung

$a_\mu \cdot a_\varrho \equiv 1 \pmod p$, also auch

$a_\mu^\nu \cdot a_\varrho^\nu \equiv 1 \pmod p$, so ist auch

$a_\mu^{\alpha+\nu} \equiv a_\varrho^{\beta-\nu} \pmod p$, womit unser Satz ausgedrückt ist.

§ 12.

Nimmt man von der Reihe der Reste der Potenzen $a_\mu^1, a_\mu^2, \ldots a_\mu^{p'}$ eine beliebige Anzahl aufeinanderfolgender heraus, so sind die Produkte je zweier gleichweit von den Enden abstehender congruent (mod. p).

Bew. Es sei eine solche Reihe $a_\mu^\nu, a_\mu^{\nu+1}, a_\mu^{\nu+2}, \ldots a_\mu^{\varrho-2}, a_\mu^{\varrho-1}, a_\mu^\varrho$, dann ist $a_\mu^{\nu+x} \cdot a_\mu^{\varrho-x} = a_\mu^{\nu+\varrho} = a_\mu^{\nu+x'} \cdot a_\mu^{\varrho-x'}$.

§ 13.

Hieran reiht sich der Satz, der eigentlich aus den Bemerkungen in § 3 im Zusammenhalte mit § 79 der disqu. arithm. folgt, jedoch der Vollständigkeit halber hier angeführt sei:

Die Summe der n^{ten} Potenzreste $a_1 + a_2 + \ldots + a_\mu$ ist immer $\equiv 0 \pmod p$.

S. dessen Verallgemeinerung in § 16!

§ 14.

Der vorausgehende Satz sowie der Satz in § 2 ergeben sich als Folgerungen aus folgendem allgemeinen:

In der Congruenz $x^n \equiv m \pmod p$ sei n ein Teiler von p—1. Sind die n Wurzeln, welche sie nach § 1 hat, $\alpha_1, \alpha_2, \ldots \alpha_n$ und bezeichnet man mit $\Sigma^t C(\alpha)$ die Summe der Combinationen der Wurzeln zur t^{ten} Klasse, so ist, wenn

$t < n$ ist, $\quad \Sigma^t C(\alpha) \equiv 0 \pmod p$, hingegen wenn

$t = n$ ist, $\quad \Sigma^n C(\alpha) = \alpha_1 \alpha_2 \ldots \alpha_n \equiv (-1)^{n-1} m \pmod p$.

Bew. Ist $f(x) \equiv 0 \pmod p$ eine Funktion n^{ten} Grades, welche n incongruente Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$ besitzt und p eine Primzahl, so ist*) $f(x) = a(x-\alpha_1)(x-\alpha_2) \ldots (x-\alpha_n) + p\psi(x)$, wo a den Coefficienten der höchsten Potenz von x in f(x) und $\psi(x)$ ein Polynom, dessen Coefficienten ganze Zahlen sind, bedeutet.

Also ist $x^n - m = (x-\alpha_1)(x-\alpha_2) \ldots (x-\alpha_n) + p\psi(x)$, daher $x^n - m \equiv x^n - \Sigma^1 C(\alpha) \cdot x^{n-1} + \Sigma^2 C(\alpha) \cdot x^{n-2} - \ldots + (-1)^n \Sigma^n C(\alpha) \pmod p$.

Diese Congruenz ist eigentlich vom $(n-1)^{ten}$ Grade, da sich beiderseits x^n weghebt, hat aber doch n Wurzeln; daher ist sie identisch. Folglich müssen die Coefficienten gleich hoher Potenzen von x beider Congruenzseiten congruent sein, also

$$\Sigma^1 C(\alpha) \equiv 0 \pmod p$$
$$\Sigma^2 C(\alpha) \equiv 0 \pmod p$$
$$\ldots \ldots \ldots \ldots$$
$$\Sigma^{n-1} C(\alpha) \equiv 0 \pmod p$$
$$\Sigma^n C(\alpha) \equiv (-1)^{n-1} m \pmod p \text{ sein.}$$

Zusatz. Setzt man hier $n = p'$ und $m = 1$, so ist

$$\Sigma^1 C(\alpha) \equiv 0 \pmod p \text{ (§ 13)}$$
$$\Sigma^{p'} C(\alpha) \equiv (-1)^{p'-1} \pmod p \text{ (§ 2).}$$

*) Lejeune Dirichlet, Vorlesungen über Zahlentheorie § 26.

§ 15.

Ist $p' = \frac{p-1}{q}$ eine gerade Zahl, so ist die Summe aller n^{ten} kleinsten positiv genommenen Potenzreste $\left(\frac{p}{2}\right) \cdot \frac{1}{q}$.

Da nämlich dieselben sich in diesem Falle nach § 4 zu Paaren gruppieren lassen, welche $= p$ sind, so ist ihre Summe $= p \cdot \frac{p-1}{2q} = \left(\frac{p}{2}\right) \cdot \frac{1}{q}$.

§ 16.

Ist γ eine beliebige ganze Zahl und sind a_1, a_2, ... $a_{p'}$ die n^{ten} Potenzreste (mod. p), so ist

$a_1^\gamma + a_2^\gamma + ... + a_{p'}^\gamma \equiv p'$ oder $\equiv 0$ (mod. p), je nachdem γ durch p' teilbar ist oder nicht.

Bew. Die n^{ten} Potenzreste sind den p' aufeinanderfolgenden Potenzen von a_μ, welches zu p' gehört, nämlich a_μ, a_μ^2, ... $a_\mu^{p'}$ (mod. p) congruent, mithin sind auch die γ^{ten} Potenzen der n^{ten} Potenzreste den γ^{ten} Potenzen jener Potenzen von a_μ (mod. p) congruent, daher sind es auch deren Summen $a_1^\gamma + a_2^\gamma + ... + a_{p'}^\gamma$ und $a_\mu^\gamma + a_\mu^{2\gamma} + ... + a_\mu^{p'\gamma}$.

Nun ist $a_\mu^\gamma + a_\mu^{2\gamma} + ... + a_\mu^{p'\gamma} \equiv 1 + a_\mu^\gamma + a_\mu^{2\gamma} + ... + a_\mu^{(p'-1)\gamma}$ (mod. p) $= \frac{a_\mu^{p'\gamma} - 1}{a_\mu^\gamma - 1}$.

$a_\mu^{p'\gamma} - 1$ ist aber ein Vielfaches von p, etwa $= mp$. Da $a_\mu^\gamma - 1$ für den Fall, dass γ nicht durch p' teilbar ist, kein Vielfaches von p ist, der Quotient $\frac{a_\mu^{p'\gamma} - 1}{a_\mu^\gamma - 1}$ aber doch eine

ganze Zahl geben muss, weil er einer Summe von ganzen Zahlen gleich ist, so muss $a_\mu^\gamma - 1$ in m enthalten sein. Also ist die Summe durch p teilbar, d. i. sie ist $\equiv 0 \pmod{p}$.

Ist γ durch p' teilbar, so ist jeder Summand dieser Summe $\equiv 1 \pmod{p}$, daher die Summe selbst $\equiv p' \pmod{p}$.

Zusatz. Als specieller Fall ist in diesem Satze der von Matrot in seinem Nouv. demonstration élémentaire du théorème de Bachet (Paris 1893) angeführte enthalten. Denn nach § 3 sind die n^{ten} Potenzreste nichts anderes als die Wurzeln der Congruenz $x^{p'} \equiv 1 \pmod{p}$ (für $p' = \frac{p-1}{q}$, wenn n und $p-1$ den grössten gemeinschaftlichen Teiler q haben). Ist nun $q = 1$, d. i. sind n und $p-1$ relative Primzahlen, so ist $p' = p-1$ und sind die n^{ten} Potenzreste die Zahlen 1, 2, . . . $(p-1)$. Wenn also γ nicht durch p teilbar ist, so folgt der genannte Satz:

$$1^\gamma + 2^\gamma + \ldots + (p-1)^\gamma \equiv 0 \pmod{p}.$$

Wäre γ etwa $= m(p-1)$, wo m eine beliebige ganze Zahl bedeutet, so sind diese einzelnen Potenzen $1^\gamma, 2^\gamma, \ldots \equiv 1$, also ihre Summe $\equiv p-1 \equiv -1 \pmod{p}$.

II. Kapitel.

Ueber binomische Congruenzen dritten Grades.

§ 1.

Hat in der Congruenz $x^3 \equiv a \pmod{p}$ p die Form $6m-1$, so ist nach § 1 Kap. I. dieselbe für jedes a möglich und giebt es nur eine reelle Wurzel, welche der Congruenz genügt. Hat p dagegen die Form $6m+1$, so ist sie nur möglich, wenn $a^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ und zwar hat sie unter dieser

Bedingung drei reelle Wurzeln. In beiden Fällen sagt man: „a ist kubischer Rest von p.“ Eine grosse Rolle spielt dieser kubische Rest, wenn p die Form $6m+1$ hat.

Nehmen wir zuerst die Congruenz

$$x^3 \equiv 1 \pmod{p}.$$

Aus dieser Congruenz folgt:

$$\text{a)}\quad x-1 \equiv 0 \pmod{p}, \text{ d. i.}$$

$$x \equiv 1 \pmod{p},$$

$$\text{b)}\quad x^2+x+1 \equiv 0 \pmod{p} \text{ oder}$$

$$x^2+x \equiv -1 \pmod{p} \text{ oder}$$

$$4x^2+4x+1 \equiv -3 \pmod{p} \text{ oder}$$

$$(2x+1)^2 \equiv -3 \pmod{p}.$$

Diese Congruenz sagt uns: „Wenn p von der Form $6m+1$ ist, so muss sie auch möglich sein, weil $x^3 \equiv 1 \pmod{p}$ in diesem Falle drei reelle Wurzeln hat, d. h.: -3 ist quadratischer Rest aller Primzahlen von der Form $6m+1$.“

Umgekehrt hat man aber auch: „Da -3 quadratischer Rest aller Primzahlen von der Form $6m+1$ ist, so ist diese Congruenz für diese Primzahl möglich, also hat die Congruenz $x^3 \equiv 1 \pmod{p}$ für $p = 6m+1$ drei reelle Wurzeln.“

Sind die drei Wurzeln der Congruenz $x^3 \equiv 1 \pmod{p}$ 1, x_1, x_2 und ist α eine Wurzel der Congruenz $x^3 \equiv a \pmod{p}$, so genügen derselben auch αx_1, αx_2. Denn es ist z. B. $(\alpha x_2)^3 = \alpha^3 x_2^3 \equiv a \pmod{p}$. Diese drei Wurzeln sind zugleich auch von einander verschieden.

Zusatz. Für die Primzahl 3, welche weder in der Form $6m+1$ noch $6m-1$ enthalten ist, findet die Congruenz $x^3 \equiv a \pmod{3}$ für jeden Wert von $a < 3$ statt.

§ 2.

Ist α eine Wurzel der Congruenz $x^3 \equiv a \pmod{p}$,

so ergeben sich die beiden anderen aus der Congruenz $(2x+\alpha)^2 \equiv -3\alpha^2 \pmod{p}$.

Bew. Ist x eine zweite Wurzel, also

$$x^3 \equiv a \pmod{p}, \text{ so ist wegen}$$

$$\alpha^3 \equiv a \pmod{p}$$

$$(x-\alpha)(x^2+\alpha x+\alpha^2) \equiv 0 \pmod{p}.$$

Da nun x und α kleiner als p vorausgesetzt werden und ungleich sind, so kann nur

$$x^2+\alpha x+\alpha^2 \equiv 0 \pmod{p} \text{ oder}$$

$$4x^2+4\alpha x+\alpha^2 \equiv -3\alpha^2 \pmod{p} \text{ oder}$$

$$(2x+\alpha)^2 \equiv -3\alpha^2 \pmod{p} \text{ sein.}$$

Z. B. eine Wurzel von $x^3 \equiv 1 \pmod{43}$ ist

$x \equiv 1 \pmod{43}$. Daher erhält man die beiden anderen aus

$$(2x+1)^2 \equiv -3 \pmod{43}.$$

Es ist $2x+1 \equiv \pm 13 \pmod{43}$, also

$$x_2 \equiv 6 \text{ und } x_3 \equiv -7 \equiv 36 \pmod{43}.$$

Von $x^3 \equiv 11 \pmod{37}$ ist

$x \equiv 21 \pmod{37}$ eine Wurzel; also ergeben sich die beiden anderen aus

$$(2x+21)^2 \equiv -1323 \equiv 9 \pmod{37}.$$

Daher erhält man $2x+21 \equiv \pm 3 \pmod{37}$, mithin

$$x_2 \equiv 28 \text{ und } x_3 \equiv 25 \pmod{37}.$$

§ 3.

Um die Wurzeln einer binomischen Congruenz dritten Grades, wenn der Modul eine Potenz einer Primzahl > 3 ist, also der Congruenz $x^3 \equiv a \pmod{p^n}$ zu bestimmen, beachte man, dass vor allem die Congruenz

$x^3 \equiv a \pmod{p}$ bestehen muss.

Denn jede Wurzel der ersteren Congruenz muss auch dieser

genügen. Diese Congruenz kann aber nach § 1 Kap. I. immer statthaben, wenn p von der Form $6m-1$ ist, weil in diesem Falle $n=3$ und $p-1$ den grössten gemeinschaftlichen Teiler 1 haben. Wenn aber p von der Form $6m+1$ ist, so wird sie nur dann stattfinden, wenn $a^{\frac{p-1}{3}} \equiv 1 \pmod{p}$. Im ersteren Falle giebt es nur eine reelle Wurzel, im letzteren deren drei.

Es lässt sich nun zeigen, dass mittels jeder Wurzel der Congruenz $x^3 \equiv a \pmod{p}$ auch jede Wurzel der Congruenz

$$x^3 \equiv a \pmod{p^n}$$ gefunden werden kann.

Denn ist α eine Wurzel der Congruenz

$$x^3 \equiv a \pmod{p^\nu}, \text{ also}$$

$$\alpha^3 \equiv a \pmod{p^\nu} \text{ oder}$$

$$\alpha^3 - a = hp^\nu \text{ und setzt man}$$

$$x = \alpha + y \cdot p^\nu, \text{ so ist}$$

$$x^3 = \alpha^3 + 3\alpha^2 y p^\nu + 3\alpha y^2 p^{2\nu} + y^3 p^{3\nu} \text{ und}$$

$$x^3 - a = \alpha^3 - a + 3\alpha^2 y p^\nu + 3\alpha y^2 p^{2\nu} + y^3 p^{3\nu} \text{ oder}$$

$$x^3 - a = hp^\nu + 3\alpha^2 y p^\nu + 3\alpha y^2 p^{2\nu} + y^3 p^{3\nu}.$$

Die beiden letzten Glieder der rechten Gleichungsseite sind aber durch $p^{\nu+1}$ teilbar, wenn $\nu \geq 1$ ist. Soll daher

$x^3 - a = (h + 3\alpha^2 y)p^\nu + 3\alpha y^2 p^{2\nu} + y^3 p^{3\nu} \equiv 0 \pmod{p^{\nu+1}}$ sein, so muss y so bestimmt werden, dass $h + 3\alpha^2 y \equiv 0 \pmod{p}$ oder

$$3\alpha^2 y \equiv -h \pmod{p}.$$

Dieses ist aber immer möglich, weil α durch p nicht teilbar ist, da ausserdem auch a durch q teilbar sein müsste gegen die Voraussetzung, d. i. für diesen Wert von y wird

$x^3 - a \equiv 0 \pmod{p^{\nu+1}}$ und die bezw. eine der drei Wurzeln der vorgelegten Congruenz ist

$$x = \alpha + yp^\nu, \text{ d. h.:}$$

Man findet mittels jeder Wurzel der Congruenz

$x^3 \equiv a \pmod{p}$ successive die Wurzeln derselben Congruenz nach den Moduln p^2, p^3, ... Da aber für $p = 6m-1$ die Congruenz

$x^3 \equiv a \pmod{p}$ für jedes beliebige durch p nicht teilbare a immer möglich ist und eine Wurzel liefert, so erhält man auf die genannte Weise auch eine Wurzel der Congruenz $x^3 \equiv a \pmod{p^n}$.

Da ferner für $p = 6m + 1$ die Congruenz

$x^3 \equiv a \pmod{p}$, wenn sie überhaupt möglich ist, drei Wurzeln hat, so erhält man auch aus jeder derselben eine Wurzel der Congruenz

$$x^3 \equiv a \pmod{p^n}.$$

Anderseits muss jede Wurzel der letzteren Congruenz auch der ersteren entsprechen, d. h. letztere hat nicht mehr Wurzeln als erstere. Man bekommt also das folgende Resultat:

Ist a durch p nicht teilbar und p von der Form $6m-1$, so ist die Congruenz $x^3 \equiv a \pmod{p^n}$ immer möglich und hat sie **eine** reelle Wurzel. Ist p von der Form $6m+1$, so ist die Congruenz $x^3 \equiv a \pmod{p^n}$ nur dann möglich, wenn $a^{\frac{p-1}{3}} \equiv 1 \pmod{p}$, und hat sie drei reelle Wurzeln. In beiden Fällen findet man sie mittels der Wurzeln der Congruenz $x^3 \equiv a \pmod{p}$.

Beispiele. 1) Die Wurzel der Congruenz

$x^3 \equiv 2 \pmod{5^2}$ ist

$x \equiv 3 \pmod{25}$.

Um eine Wurzel der Congruenz

$x^3 \equiv 2 \pmod{5^3}$ zu erhalten, setze man

$x = 3 + 25y$, so ist

$x^3 = 27 + 3.3^2.25y + 3.3.25^2y^2 + 25^3y^3$ und, da $x^3 - 2 \equiv 0 \pmod{5^3}$ sein muss, so ist

$x^3 - 2 \equiv 25 + 3.3^2.25y \pmod{5^3}$ oder

$$\equiv (1 + 27y) . 25 \pmod{5^3}.$$

Bestimmt man y aus

$1 + 27y \equiv 0 \pmod 5$, also

$2y \equiv -1$ oder $y \equiv 2 \pmod 5$, so erhält man $x \equiv 3 + 50 = 53 \pmod{5^3}$.

In der That ist

$$53^3 \equiv 2 \pmod{5^3}.$$

2) Es soll eine Wurzel der Congruenz

$x^3 \equiv 48 \pmod{7^2}$ gesucht werden. Die Congruenz

$x^3 \equiv 48 \equiv 6 \pmod 7$ ist möglich, da 6 ein kubischer Rest von 7 ist, und zwar ist

$x \equiv 3 \pmod 7$ eine Wurzel dieser Congruenz. Setzt man daher

$x = 3 + 7y$, so ist

$$x^3 - 48 = 27 - 48 + 3.3^2.7y + 3.3.7^2y^2 + 7^3y^3$$

oder $x^3 - 48 \equiv (-3 + 27y) . 7 \pmod{7^2}$.

Aus $27y \equiv 3 \pmod 7$ oder

$6y \equiv 3 \pmod 7$ erhält man

$y \equiv 4 \pmod 7$.

Mithin ist $x \equiv 3 + 28 = 31 \pmod{7^2}$ eine Wurzel der Congruenz $x^3 \equiv 48 \pmod{7^2}$.

Es ist auch $31^3 \equiv 48 \pmod{7^2}$.

§ 4.

Ueber die Anzahl der kubischen durch p nicht teilbaren Reste $(\mathrm{mod}.\, p^n)$ ist Folgendes zu bemerken.

Wenn p die Form $6m - 1$ hat, so ist jede der $\varphi(p^n) = (p - 1)p^{n-1}$ durch p nicht teilbaren Zahlen, welche kleiner als p sind, kubischer Rest $(\mathrm{mod}.\, p^n)$. Wenn p hingegen die Form $6m + 1$ hat, so sei α ein kubischer Rest $(\mathrm{mod}.\, p)$. Dann sind alle Zahlen von der Form

$\alpha + hp$, wo h die Werte 0, 1, 2, . . . $(p^{n-1}-1)$ hat, kubische Reste (mod. p^n), ermöglichen also die Congruenz $x^3 \equiv a \pmod{p^n}$, wenn a die Form $\alpha + hp$ hat. Denn jede Wurzel dieser Congruenz ist auch Wurzel der Congruenz $x^3 \equiv a \pmod{p}$ und dieser Congruenz kann entsprochen werden durch alle Werte von $a = \alpha + hp$, wo h den oben angegebenen Zahlenraum umfasst. Die Anzahl der Werte von a ist aber, weil es $\frac{1}{3}(p-1)$ kubische Reste (mod. p) — α — giebt und zu jedem derselben p^{n-1} Werte von h gehören, $= \frac{1}{3}(p-1)p^{n-1}$. Daher können für $x^3 \equiv a \pmod{p^n}$ höchstens $\frac{1}{3}(p-1)p^{n-1}$ kubische Reste sich ergeben.

So viele müssen es aber auch wenigstens sein. Denn die Congruenz $x^3 \equiv a \pmod{p^n}$ kann nach § 3 nicht mehr als drei incongruente Wurzeln haben. Also müssen von den Resten der $(p-1)p^{n-1}$ durch p nicht teilbaren Potenzen $1^3, 2^3, \ldots . (p^n-1)^3 \pmod{p^n}$ höchstens immer je drei einander gleich und die Anzahl der kubischen Reste (mod. p^n) wenigstens $= \frac{1}{3}(p-1)p^{n-1}$ sein.

Daher ist die Anzahl aller durch p nicht teilbaren kubischen Reste (mod. p^n), wenn p von der Form $6m+1$ ist, $= \frac{p-1}{3}p^{n-1}$.*)

Ist a durch p teilbar, so kann es nur dann kubischer Rest (mod. p^n) sein, wenn es von der Form $a_1 p^{3\nu}$ ist, wo a_1

*) Ueber die Anzahl der kubischen Reste (mod. p^n) hat Kummer einige Bemerkungen in seiner Habilitationsschrift gemacht, deren Original den Titel führt: „De residuis cubicis disquisitiones nonnullae analyticae, quas auctoritate amplissimi philosophorum ordinis in Academia Vratislaviensi pro loco professoris publici ordinarii rite obtinendo die XXVI. m. octobr. 1842. publice defendet Ernestus Eduardus Kummer phil. Dr. Prof. publ. ord. des.“ Leider ist selbes reich an Druckfehlern. Auch im Abdrucke dieser Schrift im XXXII. Bande von Crelle's Journal finden sich solche ziemlich zahlreich.

die Primzahl p nicht enthält. Dann stimmt die Anzahl der kubischen Reste der Congruenz $x^3 \equiv a \pmod{p^n}$ überein mit der Anzahl der kubischen Reste von $x_1^3 \equiv a_1 \pmod{p^{n-3\nu}}$.

$x^3 \equiv a \pmod{p^n}$ hat in diesem Falle $p^{2\nu}$ bezw. $3.p^{2\nu}$ incongruente Wurzeln (mod. p^n), je nachdem p die Form $6m-1$ oder $6m+1$ hat. Denn ist α eine Wurzel der Congruenz $x_1^3 \equiv a_1 \pmod{p^{n-3\nu}}$, so sind αp^ν, $(\alpha + p^{n-3\nu})p^\nu$, $(\alpha + 2p^{n-3\nu})p^\nu$, ... $[\alpha + (p^{2\nu} - 1)p^{n-3\nu}]p^\nu$ Wurzeln der Congruenz $x^3 \equiv a \pmod{p^n}$.

1) Sind die Coefficienten von $p^{n-3\nu}$ in zweien dieser Ausdrücke h und h_1, dann ist

$$(\alpha + hp^{n-3\nu})p^\nu \equiv (\alpha + h_1 p^{n-3\nu})p^\nu \pmod{p^n}$$

oder es sind zwei Wurzeln gleich, wenn

$$(h - h_1)\, p^{n-3\nu} \equiv 0 \pmod{p^{n-\nu}} \text{ oder}$$

$$h - h_1 \equiv 0 \pmod{p^{2\nu}}.$$

Also muss $h \leqq p^{2\nu} - 1$ sein. In der That giebt auch

$$[\alpha + (p^{2\nu} - 1)\, p^{n-3\nu}]p^\nu$$

eine Zahl, welche kleiner als p^n und

$$[\alpha + p^{2\nu} \cdot p^{n-3\nu}]p^\nu$$

eine solche, welche grösser als p^n ist, wie man sich leicht überzeugen kann.

2) Ist h irgend einer dieser Coefficienten von $p^{n-3\nu}$ in den oben angegebenen Ausdrücken, so ist

$$[(\alpha + hp^{n-3\nu})p^\nu]^3 = \alpha^3 p^{3\nu} + 3\alpha^2 hp^n + 3\alpha h^2 p^{2n-3\nu} + h^3 p^{3n-6\nu}$$

$$\equiv \alpha^3 p^{3\nu} \pmod{p^n} \text{ für } 2n - 3\nu \geqq n \text{ oder}$$

$$n \geqq 3\nu \text{ oder}$$

$$\nu \leqq \frac{n}{3}, \text{ was}$$

immer Voraussetzung ist.

Z. B. mittels der Wurzel $x \equiv 5 \pmod 7$ der Congruenz $x^3 \equiv 6 \pmod 7$ findet man nach dem im § 3 angegebenen Verfahren eine Wurzel der Congruenz

$$x^3 \equiv 6 \pmod{7^2}, \text{ nämlich}$$

$$x \equiv 40 \pmod{7^2}.$$

Daher sind z. B. die $7^4 = 2401 \pmod{7^8}$ incongruenten Ausdrücke $40 . 7^2$, $(40 + 1 . 7^2)\, 7^2$, $(40 + 2 . 7^2)\, 7^2$, ... $[40 + (7^4 - 1)\, 7^2]\, 7^2$ Wurzeln der Congruenz $x^3 \equiv 6 . 7^6 \pmod{7^8}$. In der That ist z. B. $\{[40 + (7^4 - 1)\, 7^2]\, 7^2\}^3 \equiv 7^6 . 6 \pmod{7^8}$ oder wieder $40^3 \equiv 6 \pmod{7^2}$.

§ 5.

Die Fälle $p^n = 3^n$ und $p^n = 2^n$ erfordern eine besondere Betrachtung.

Zur Bestimmung der Wurzeln der Congruenz $x^3 \equiv a \pmod{3^{n+1}}$, wobei a als nicht durch 3 teilbar vorausgesetzt wird, mittels der Wurzeln von

$$x^3 \equiv a \pmod 3$$

verlangt die unter § 3 angegebene Methode eine Modifikation, weil man auf die Auflösung der Congruenz

$$3\alpha^2 y \equiv -h \pmod 3 \text{ kommt.}$$

Ist h durch 3 teilbar, so ist das α, welches der Congruenz $x^3 \equiv a \pmod{3^n}$ genügt, auch zugleich eine Wurzel der Congruenz $x^3 \equiv a \pmod{3^{n+1}}$.

Z. B. $23^3 \equiv 17 \pmod{3^3}$ und

$\equiv 17 \pmod{3^4}$, weil

$$23^3 - 17 = 450 . 27.$$

Ist h durch 3 nicht teilbar, so setze man, wenn

$x \equiv \alpha \pmod{3^n}$ eine Wurzel der Con-

gruenz $x^3 \equiv a \pmod{3^n}$ ist,

$x = \alpha + 3^{n-1}y$. Dann hat man

$$x^3 - a = \alpha^3 - a + 3^n\alpha^2 y + 3^{2n-1}\alpha y^2 + 3^{3n-3}y^3$$

und $x^3 - a \equiv \alpha^3 - a + 3^n\alpha^2 y \pmod{3^{n+1}}$ für

$2n - 1 \gtreqless n + 1$ oder

$n \gtreqless 2$.

Setzt man $\alpha^3 - a \equiv h.3^n$, so ist

$x^3 - a \equiv (h + \alpha^2 y)3^n \pmod{3^{n+1}}$, d. i.

bestimmt man y aus $h + \alpha^2 y \equiv 0 \pmod 3$, so ist

$x = \alpha + 3^{n-1}y$ eine Wurzel der Congruenz $x^3 \equiv a \pmod{3^{n+1}}$.

Z. B. eine Wurzel der Congruenz

$x^3 \equiv 17 \pmod{3^3}$ ist auch

$x \equiv 5 \pmod{3^3}$.

Setzt man $x = 5 + 9y$, so erhält man

$y \equiv 2 \pmod 3$, mithin

$x \equiv 5 + 2.9 \equiv 23 \pmod{3^4}$ als eine Wurzel der Congruenz $x^3 \equiv 17 \pmod{3^4}$.

Dass aber die Congruenz $x^3 \equiv a \pmod{3^n}$ für $n \geqq 2$ drei incongruente Wurzeln hat, lässt sich auf dem Wege der Induktion folgendermassen beweisen:

Aus jeder Wurzel der Congruenz

$x^3 \equiv a \pmod{3^n}$ lässt sich nach dem Vorausgehenden eine Wurzel der Congruenz

$x^3 \equiv a \pmod{3^{n+1}}$ ableiten. Daher hat letztere Congruenz mindestens ebenso viele Wurzeln als erstere. Andererseits ist aber jede Wurzel der letzteren auch eine solche der ersteren.

Also hat $x^3 \equiv a \pmod{3^{n+1}}$ ebenso viele Wur-

zeln als $x^3 \equiv a \pmod{3^n}$.

Nun hat $x^3 \equiv a \pmod 9$ drei Wurzeln, nämlich für $a = 1$ die Wurzeln 1, 4 und 7, für $a = 8$ die Wurzeln 2, 5 und 8. Mithin hat die Congruenz

$$x^3 \equiv a \pmod{3^n} \text{ für } n \geqq 2$$ drei incongruente Wurzeln.

Mittels einer derselben, α, lassen sich die beiden übrigen finden. Es sei also x irgend eine der anderen, so dass $\alpha^3 \equiv a \pmod{3^n}$ und

$$x^3 \equiv a \pmod{3^n}, \text{ so ist}$$

$$x^3 - \alpha^3 = (x-\alpha)(x^2 + \alpha x + \alpha^2) \equiv 0 \pmod{3^n}.$$

Nun müssen α und x von derselben Form wie a, nämlich zugleich von der Form $3m+1$ oder $3m-1$ sein, da ausserdem, wie man sich leicht überzeugen kann, nicht

$$\alpha^3 - a \equiv 0 \pmod{3^n} \text{ sein könnte.}$$

Dann ist $x - \alpha \equiv 0 \pmod 3$, aber auch

$$x^2 + \alpha x + \alpha^2 \equiv 0 \pmod 3, \text{ also}$$

$$\frac{x-\alpha}{3} \cdot \frac{x^2 + \alpha x + \alpha^2}{3} \equiv 0 \pmod{3^{n-2}}.$$

Da aber $x^2 + \alpha x + \alpha^2$ entweder

$= 9(m^2 + m m_1 + m_1^2) + 6(m + m_1) + 3(m + m_1) + 3$ oder

$= 9(m^2 + m m_1 + m_1^2) - 6(m + m_1) - 3(m + m_1) + 3$, je nachdem α und x von der Form $3m+1$ und $3m_1+1$ oder $3m-1$ und $3m_1-1$ sind, so kann es nur durch 3 teilbar sein. Daher ist $\frac{x-\alpha}{3} \equiv 0 \pmod{3^{n-2}}$, folglich

$$x \equiv \alpha \pmod{3^{n-1}}.$$

Mithin sind die beiden Wurzeln ausser α noch $\alpha \pm 3^{n-1}$ und $\alpha \pm 2 \cdot 3^{n-1}$ d. h. entweder $\alpha + 3^{n-1}$ und $\alpha + 2 \cdot 3^{n-1}$

oder $\alpha - 3^{n-1}$ und $\alpha + 3^{n-1}$

oder $\alpha - 3^{n-1}$ und $\alpha - 2 \cdot 3^{n-1}$.

Z. B. ist $19^3 \equiv (19 + 3^3)^3 \equiv (19 + 2.3^3)^3 \equiv 55 \pmod{3^4}$.

Die eine dieser drei Wurzeln von $x^3 \equiv a \pmod{3^n}$ ist immer zugleich auch eine Wurzel der Congruenz $x^3 \equiv a \pmod{3^{n+1}}$.

Es sei die kleinste derselben α. Wenn nicht $\alpha^3 - a \equiv 0 \pmod{3^{n+1}}$, so ist entweder $(\alpha + 3^{n-1})^3 - a$ oder $(\alpha + 2 \cdot 3^{n-1})^3 - a \equiv 0 \pmod{3^{n+1}}$. Wenn $\alpha^3 - a$ nicht $\equiv 0 \pmod{3^{n+1}}$, so ist es von der Form $(3m \pm 1)3^n$. Dann ist $(\alpha + 3^{n-1})^3 - a = \alpha^3 + 3^n\alpha^2 + 3^{2n-1}\alpha + 3^{3n-3} - a \equiv (3m \pm 1)\, 3^n + 3^n\alpha^2 + 3^{2n-1}\alpha + 3^{3n-3} = 3^{n+1}m + 3^{2n-1}\alpha + 3^{3n-3} + 3^n(\alpha^2 \pm 1) \equiv (\alpha^2 \pm 1)\, 3^n \pmod{3^{n+1}}$ für $2n - 1 \gtrless n + 1$ oder

$$n \gtrless 2,$$

$(\alpha + 2.3^{n-1})^3 - a = \alpha^3 + 2.3^n\alpha^2 + 2^2.3^{2n-1}\alpha + 2^3.3^{3n-3} - a \equiv (2\alpha^2 \pm 1)3^n \pmod{3^{n+1}}$ unter den gleichen Bedingungen für den Wert von n.

Weil nun $\alpha = 3k \pm 1$, so ist α^2 von der Form $3k + 1$, mithin $\alpha^2 \pm 1 = 3k + 2$ oder $= 3k$ und bzw.

$2\alpha^2 \pm 1 = 6k + 3$ oder $= 6k + 1$, also

entweder $\alpha^2 \pm 1 \equiv 0 \pmod 3$ oder $2\alpha^2 \pm 1 \equiv 0 \pmod 3$.

Setzt man dann die Wurzel der Congruenz $x^3 \equiv a \pmod{3^{n+1}}$, welche zugleich Wurzel der Congruenz $x^3 \equiv a \pmod{3^n}$ ist, $= \alpha_1$, so sind die beiden anderen $\alpha_1 \pm 3^n$ und $\alpha_1 \pm 2 \cdot 3^n$.

Z. B. als eine Wurzel der Congruenz

$x^3 \equiv 64 \pmod{3^4}$ erhält man aus

$x^3 \equiv 64 \pmod{3^3}$ oder

$x^3 \equiv 10 \pmod{3^3}$, da eine solche der letzteren

$x \equiv 31 \pmod{3^3}$ ist,

$x \equiv 31 \pmod{3^4}$.

Daher sind die beiden anderen $31 - 3^3 = 4$ und $31 + 3^3 = 58$.

Weil die Congruenz $x^3 \equiv a \pmod{3^n}$ drei incongruente Wurzeln hat, so ergiebt sich dann wie oben in § 4 für $p = 6m+1$, dass die Anzahl der kubischen durch 3 nicht teilbaren Reste $= \frac{p-1}{3} \cdot p^{n-3} = 2 \cdot 3^{n-2}$ ist. Im Besonderen ist zu bemerken, dass alle diese kubischen Reste die Form $9m \pm 1$ haben. Denn alle durch 3 nicht teilbaren Zahlen sind von der Form $3m \pm 1$. Diese geben zum Kubus erhoben $27m^3 \pm 27m^2 + 9m \pm 1$ d. i. Zahlen von der Form $9m \pm 1$. Also haben alle kubischen Reste die eine oder andere dieser Formen. Zugleich giebt der Umstand, dass die Anzahl der Zahlen dieser Formen, welche kleiner als 3^n sind, $= 2 \cdot 3^{n-2}$ ist, eine Bestätigung der vorstehenden Behauptung über die Anzahl der kubischen durch 3 nicht teilbaren Reste $(\mathrm{mod.}\, 3^n)$.

Dass auch Zahlen, welche den Faktor $3^{3\nu}$ enthalten, als kubische Reste $(\mathrm{mod.}\, 3^n)$ betrachtet werden können und zwar dass jeder solche Rest zu $3^{2\nu} \cdot 3 = 3^{3\nu}$ Wurzeln der Congruenz $x^3 \equiv a \pmod{3^n}$ gehört, kann ebenso wie in § 4 für $p = 6m \pm 1$ gefolgert werden.

§ 6.

Es sei $p^n = 2^n$. Aus jeder Wurzel α der Congruenz $x^3 \equiv a \pmod{2^n}$, wo a als ungerade vorausgesetzt wird, erhält man eine, aber auch nur eine Wurzel der Congruenz $x^3 \equiv a \pmod{2^{n+1}}$, wenn man $x \equiv \alpha + 2^n \pmod{2^{n+1}}$ nimmt.

Denn setzt man $x = \alpha + 2^n y$, so findet man nach dem in den §§ 3 und 5 angewendeten Verfahren, dass $y = 1$ oder $= 0$ sein muss. Letzteres findet statt, wenn in $\alpha^3 - a = h.2^n$ h eine gerade Zahl ist. Dann ist α auch eine Wurzel der Congruenz $x^3 \equiv a \pmod{2^{n+1}}$. Denn $(\alpha + 2^n)^3$ wäre in diesem Falle $\equiv a + 2^n \pmod{2^{n+1}}$. Man findet nämlich leicht nach einigen Reduktionen, dass

$$(\alpha + 2^n)^3 \equiv \alpha^3 + \alpha^2 . 2^n \pmod{2^{n+1}}, \text{ also}$$
$$(\alpha + 2^n)^3 - a \equiv \alpha^3 - a + \alpha^2 . 2^n \pmod{2^{n+1}}.$$

Ist nun $h = 2k$, so ist

$$(\alpha + 2^n)^3 - a \equiv 2^{n+1} k + \alpha^2 . 2^n \pmod{2^{n+1}}$$
$$\equiv \alpha^2 . 2^n \pmod{2^{n+1}}.$$

Da jedoch α immer eine ungerade Zahl $= 2k_1 + 1$, so ist $\alpha^2 = (2k_1 + 1)^2 \equiv 1 \pmod 4$, mithin

$$(\alpha + 2^n)^3 - a \equiv 2^n \pmod{2^{n+1}} \text{ oder}$$
$$(\alpha + 2^n)^3 \equiv a + 2^n \pmod{2^{n+1}}.$$

Jede Wurzel der Congruenz $x^3 \equiv a \pmod{2^{n+1}}$ muss aber auch der Congruenz $x^3 \equiv a \pmod{2^n}$ genügen.

$x^3 \equiv a \pmod 4$ hat aber nur eine Wurzel, nämlich für $a = 1, 3$ bzw. 1, 3. Also besitzt die Congruenz $x^3 \equiv a \pmod{2^n}$ auch nur eine Wurzel.

Von den Resten der Kuben der ungeraden Zahlen $1^3, 3^3, 5^3, \ldots . (2^n - 1)^3 \pmod{2^n}$ sind also keine zwei einander gleich. Daher ist die Anzahl der kubischen durch 2 nicht teilbaren Reste $\pmod{2^n} = 2^{n-1}$.

Ueber die durch $2^{3\nu}$ teilbaren kubischen Reste $\pmod{2^n}$ gelten die in § 4 durchgeführten Auseinandersetzungen.

Zusatz. Da man jede ungerade Zahl in der Form $2^\nu k \pm 1$, wo k den Faktor 2 nicht enthält, darstellen kann, so ist

$(2^{\nu}k \pm 1)^3 \equiv 3 \cdot 2^{\nu}k \pm 1 \pmod{2^n}$ für $n \geqq 2\nu$,

$\equiv 2^{\nu}k \pm 1 \pmod{2^n}$, wenn $\nu = n-1$ oder $= n$ ist. Daher sind nach den Moduln 4 und 8 die Kuben der ungeraden Zahlen sich selbst congruent. Nach dem Modul 64 z. B. ist $31^3 \equiv 31$

$33^3 \equiv 33$

$63^3 \equiv 63$ u. s. w.

§ 7.

Sind die Wurzeln der Congruenz $x^3 \equiv m \pmod{P}$, wo P das Produkt der Primzahlpotenzen 2^{λ}, 3^{μ}, $p_1^{\nu_1}$, $p_2^{\nu_2}$, ... , λ, ν_1, r_2, . . . 0 und jede beliebige ganze Zahl, μ aber $\geqq 2$ sei, zu suchen, so ist die Congruenz nur dann möglich, wenn $x^3 \equiv m$ nach jeder dieser Primzahlpotenzen möglich ist. Sind dann σ

τ_1, τ_2, τ_3

$\alpha_1, \alpha_2, \alpha_3$

$\beta_1, \beta_2, \beta_3$

. . . . . .

bzw. die Wurzeln der Congruenzen:

$x^3 \equiv m \pmod{2^{\lambda}}$

$x^3 \equiv m \pmod{3^{\mu}}$

$x^3 \equiv m \pmod{p_1^{\nu_1}}$

$x^3 \equiv m \pmod{p_2^{\nu_2}}$

. . . . . .

und bestimmt man die Zahlen, welche zugleich $\equiv \sigma \pmod{2^{\lambda}}$, $\equiv \tau_1, \tau_2, \tau_3 \pmod{3^{\mu}}$, $\equiv \alpha_1, \alpha_2, \alpha_3 \pmod{p_1^{\nu_1}}$, $\equiv \beta_1, \beta_2, \beta_3 \pmod{p_2^{\nu_2}}$, ... , so sind diese die Wurzeln der vorgelegten Congruenz. Um sie zu finden, setze man

$P = 2^{\lambda} \cdot P' = 3^{\mu} \cdot P'' = p_1^{\nu_1} \cdot P_1 = p_2^{\nu_2} \cdot P_2 = \ldots$, und bestimmt

man die Werte $a', a'', a_1, a_2, \ldots$, welche die Congruenzen

$$P'.a' \equiv 1 \pmod{2^\lambda}$$
$$P''.a'' \equiv 1 \pmod{3^\mu}$$
$$P_1.a_1 \equiv 1 \pmod{p_1^{\nu_1}}$$
$$P_2.a_2 \equiv 1 \pmod{p_2^{\nu_2}}$$
$$\ldots\ldots\ldots$$

befriedigen. Alsdann sind dieselben enthalten in dem Ausdrucke $x \equiv P'a'\sigma + P''a''\tau + P_1a_1\alpha + P_2a_2\beta + \ldots$ (mod. P), wenn man für $\tau, \alpha, \beta, \ldots$ nacheinander bezw. $\tau_1, \tau_2, \tau_3; \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3, \ldots\ldots$ setzt und in diesem Ausdrucke die Zahlen dieser Gruppen auf alle mögliche Weise kombiniert. Denn derselbe ist $\equiv \sigma \pmod{2^\lambda}$, weil $P'', P_1, P_2, \ldots$ durch $2^\lambda, \equiv \tau \pmod{3^\mu}$, weil $P', P_1, P_2, \ldots$ durch $3^\mu, \ldots\ldots$ teilbar sind; daher sind auch dessen dritte Potenzen $\equiv \sigma^3, \tau^3, \alpha^3, \ldots\ldots \equiv m$ bzw. nach den Moduln $2^\lambda, 3^\mu, p_1^{\nu_1}, p_2^{\nu_2}, \ldots$, mithin, weil $2^\lambda, 3^\mu, p_1^{\nu_1}, p_2^{\nu_2}, \ldots$ relative Primzahlen sind, auch $\equiv m \pmod{2^\lambda 3^\mu p_1^{\nu_1} p_2^{\nu_2} \ldots}$.

Zusatz. Die Anzahl der Wurzeln ist, wenn n die Anzahl der Primfaktoren $3, p_1, p_2, \ldots$ und $\mu \geqq 2$ ist, $= 3^n$, hingegen $= 3^{n-1}$, wenn $\mu = 1$ oder $= 0$ ist.

Beispiel. Von $x^3 \equiv 1 \pmod{91}$ sind die Wurzeln 1, 9, 16, 22, 29, 53, 74, 79, 81, weil die Wurzeln von

$x^3 \equiv 1 \pmod 7$ 1, 2 und 4,

von $x^3 \equiv 1 \pmod{13}$ 1, 3 und 9 sind.

§ 8.

Unter den kubischen Resten einer Primzahl $p = 6m + 1$ ist derjenige besonders bemerkenswert, welchem die dritten Potenzen jener Zahlen congruent sind, die p in der Form

x^2+xy+y^2 darstellen. Ist a dieser kubische Rest, so dass

$$x^3 \equiv y^3 \equiv a \pmod{p} \text{ und}$$

$x^2+xy+y^2=p$, so stellen auch x und $-(x+y)$ sowie y und $-(x+y)$ p in dieser Form dar. Denn $x^2+x[-(x+y)]+[-(x+y)]^2=x^2+xy+y^2$ u. s. w. Dieses $-(x+y)$ ist nach § 8 die dritte Wurzel der Congruenz $x^3 \equiv a \pmod{p}$, wenn x und y die beiden ersten sind.

Umgekehrt: Stellen x und y p in der Form x^2+xy+y^2 dar, so ist $x^3 \equiv y^3$ etwa $\equiv a \pmod{p}$ und $-(x+y)$ die dritte darstellende Zahl und zugleich die dritte Wurzel der Congruenz $x^3 \equiv a \pmod{p}$.

Zusatz. Daraus folgt, dass $p=6m+1$ nur auf drei verschiedene Arten in der Form x^2+xy+y^2 dargestellt werden kann. Denn gäbe es noch eine vierte darstellende Zahl z, so dass

$x^2+xz+z^2=p$, so müsste

$x^3 \equiv z^3 \pmod{p}$, also auch z eine Wurzel der Congruenz $x^3 \equiv a \pmod{p}$ sein, was unmöglich ist.*)

§ 9.

Ist $x=m$ eine darstellende Zahl und y eine zweite zu suchende, also $m^2+my+y^2=p$, so ist

$$y=\frac{-m \pm \sqrt{4p-3m^2}}{2} \text{ d. i.}$$

$\frac{-m+\sqrt{4p-3m^2}}{2}$ und $\frac{-m-\sqrt{4p-3m^2}}{2}$ sind die beiden anderen darstellenden Zahlen und $4p-3m^2$ ist ein Quadrat.

*) S. hierüber „Vorlesungen über Zahlentheorie von Lejeune Dirichlet, herausgg. von Dedekind, § 70, wo dasselbe Resultat mittels der Theorie der quadr. Formen gefunden ist.

Umgekehrt: Ist $4p-3m^2$ ein Quadrat, etwa $=v^2$, so ist m eine der darstellenden Zahlen, während die beiden anderen $\frac{-m+v}{2}$ und $\frac{-m-v}{2}$ sind.

In der That ist z. B.

$$m^2+m.\frac{-m+v}{2}+\left(\frac{-m+v}{2}\right)^2=\frac{3m^2+v^2}{4}=p.$$

Zusatz. Ist 1 eine der darstellenden Zahlen, so ist $4p-3$ ein Quadrat. Umgekehrt: Ist $4p-3$ ein Quadrat, so ist 1 eine der darstellenden Zahlen. Die beiden anderen findet man auch nach § 1.

§ 10.

Um diese darstellenden Zahlen zu finden, setze man in dem Ausdrucke $4p-3m^2$ für m nach und nach die Werte 1, 2, 3, . . . , bis $4p-3m^2$ ein Quadrat wird. Auf diese Weise findet man schneller speziell diese darstellenden Zahlen als mittels der Theorie der quadratischen Formen.

Z. B. für $p=19$ hat man: $4p-3m^2=76-3m^2$. Für $m=2$ ist $4p-3m^2=64=v^2$, also $v=8$.

Daher sind die drei darstellenden Zahlen: $m=2$

$$\frac{-m+v}{2}=3$$

$$\frac{-m-v}{2}=-5.$$

In der That ist: $19=2^2+2.3+3^2$

$$=2^2+2(-5)+(-5)^2$$

$$=3^2+3(-5)+(-5)^2.$$

Für $p=31$ ist $4p-3m^2=124-3m^2$. Für $m=1$ ist $4p-3m^2=121=v^2$, also $v=11$.

Mithin sind die drei darstellenden Zahlen: $m=1$

$$\frac{-m+v}{2}=5$$

$$\frac{-m-v}{2}=-6.$$

Thatsächlich ist: $31=1^2+1.5+5^2$

$$=1^2+1(-6)+(-6)^2$$

$$=5^2+5(-6)+(-6)^2.$$

Diese Zahlen, welche p in der Form x^2+xy+y^2 oder, weil immer eine derselben, nämlich $\frac{-m-v}{2}$ negativ ist, in der Form x^2-xy+y^2 darstellen, sind desswegen von grosser Wichtigkeit, weil die Theorie der kubischen Reste auf den complexen Zahlen von der Form $a+b\varrho$ beruht, wo $\varrho=\frac{-1+\sqrt{-3}}{2}$, d. i. eine der beiden imaginären Kubikwurzeln der Einheit ist. Setzt man

$a+b\varrho=a+b.\frac{-1+\sqrt{-3}}{2}$, so ist

$a+b\varrho^2=a+b.\frac{-1-\sqrt{-3}}{2}$ und

$(a+b\varrho)(a+b\varrho^2)=a^2-ab+b^2$.